

The listing of claims will replace all prior versions, and listings, of claims in the application:

**Listing of Claims:**

1. (Canceled)
2. (Currently amended) A method of providing an award on a network of gaming machines comprising:
  - encrypting a server-initiated message on the network at a server with a key pair that is generated using a setup key stored both in memory associated with the server and in memory associated with a gaming machine wherein the setup key is removed from the memory associated with the gaming machine after generation of the key pair;
  - transmitting the message to one of the gaming machines to establish communications with the gaming machine;
  - decrypting the message at the gaming machine with the key pair; and
  - paying an award at the gaming machine responsive to the message.
3. (Previously presented) The method of claim 2 wherein the key pair is a private key pair.
4. (Previously presented) The method of claim 2 wherein encrypting the message comprises signing the message.
5. (Previously presented) The method of claim 2 wherein encrypting the message comprises verifying the message.
6. (Previously presented) The method of claim 2 wherein encrypting the message comprises both signing and verifying the message.
7. (Previously presented) The method of claim 3 wherein said method further comprises periodically changing the private key pair.
8. (Previously presented) The method of claim 7 wherein said method further comprises identifying the private key pair that encrypted the message.

9. (Previously presented) The method of claim 8 wherein identifying the private key pair comprises associating a session number with each private key pair.

10. (Currently amended) A method for encrypting communications on a network of gaming machines comprising:

establishing first key at a first node associated with a gaming machine;

establishing a second key at a second node on the network associated with a server remote from the gaming machine wherein the first key and the second key are generated using a setup key stored both in memory associated with the first node and in memory associated with the second node wherein the setup key is removed from the memory associated with the first node after generation of the first key and the second key;

encrypting a server-initiated award payment message at the second node with the second key;

transmitting the award payment message to the first node with the first key as a first communication between the first and second nodes; and

decrypting the award payment message at the first node and operating upon the message at the first node to pay an award at the gaming machine responsive to the award payment message.

11. (Previously presented) The method of claim 10 wherein a message originates at the first node and includes data indicating an amount played at the gaming machine.

12. (Previously presented) The method of claim 11 wherein said second node is associated with a network computer that receives messages from multiple gaming machines on the network, said messages each including data indicating an amount played on one of the gaming machines.

13. (Previously presented) The method of claim 10 wherein the encrypting a message and decrypting the message is accomplished with a private key pair.

14. (Previously presented) The method of claim 10 wherein encrypting the award payment message comprises signing the message.

15. (Previously presented) The method of claim 10 wherein encrypting the award payment message comprises verifying the message.

16. (Previously presented) The method of claim 10 wherein encrypting the award payment message comprises both signing and verifying the message.
17. (Previously presented) The method of claim 13 wherein said method further comprises periodically changing the private key pair.
18. (Previously presented) The method of claim 17 wherein said method further comprises identifying the private key pair that encrypted the message.
19. (Previously presented) The method of claim 18 wherein identifying the private key pair comprises associating a session number with each private key pair.
20. (Previously presented) The method of claim 10 wherein the award payment message originates at the second node and includes data indicating a bonus payable at the gaming machine.
21. (Currently amended) A network of gaming machines comprising:
  - a first node associated with a gaming machine on the network;
  - a second node located on the network and associated with a server remote from the first node to transmit server initiated award payment messages and establish communications with the first node;
  - a key pair, one key being associated with the first node and the other key being associated with the second node, the key pair configured to be generated using a setup key stored both in memory associated with the first node and in memory associated with the second node wherein the setup key is configured to be removed from the memory associated with the first node after generation of the key pair;
  - a process operable at each node to encrypt messages between the nodes using the key pair; and
  - a process operable at the first node to decrypt, using the key pair, the award payment messages from the second node for paying awards at the gaming machine responsive to the award payment ~~messenges~~ messages.

22. (Previously presented) The network of claim 21 wherein said key pair comprises a private key pair.

23. (Previously presented) The network of claim 22 wherein said key pair is periodically changed and wherein said network further comprises a process operable to identify each key pair.